

Multilayer crypto method using playing cards shuffling operation

Rashad J. Rasras¹, Mutaz Rasmi Abu Sara², Ziad Alqadi¹

¹Department of Electrical Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan

²Department of Information Technology, Faculty of Engineering and Information Technology, Palestine Ahliya University, Bethlehem, Palestine

Article Info

Article history:

Received Aug 21, 2024

Revised Dec 9, 2024

Accepted Dec 25, 2024

Keywords:

Blocking

Layer

Private key

Shuffling

Shuffling back

ABSTRACT

An efficient and highly secure method of secret message cryptography will be presented which based on the principle of playing cards shuffling. The method will be implemented in a selected number of layers, each layer will encrypt-decrypt the input message using its own private key (PK), the output of any layer can be taken as a final encrypted-decrypt message, increasing the number of layers will increase the security level of the message, making the hacking attacks impossible. In the encryption function a key generation and a message blocks shuffling will be executed, while in the decryption function the key generation and the message blocks reverse shuffling will be executed. The PK used in this method will be complicated and it will contain for each layer 2 chaotic parameters (r and x) and the block size (BS), utilizing these parameters, a chaotic logistic map model is run to produce a chaotic key, which is sorted to produce the layer's index key. Applying 4 layers the length of confidential key will be 768 bits, this length will be able to generate a large key space which is robust to hacking attempts. The speed parameters and throughput of the proposed will be calculated and compared with those of other methods.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Rashad J. Rasras

Department of Electrical Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University
Amman 11134, P.O. Box 15008, Jordan

Email: rashad.rasras@bau.edu.jo

1. INTRODUCTION

Scrambling playing cards leads to scrambling and redistributing the cards, and the more scrambling, the greater the degree of irregularity and sequence of these cards. There are $52! \approx 2^{225.58}$ ways to mix a deck of cards. Hence, a cipher created from a deck of cards has the potential to emulate the security of many computer ciphers. Analysis of existing playing cards crypto systems [1]-[3] showed that most of card ciphers are stream ciphers which encrypt one letter at a time. A lot of methods for data cryptography were introduced by various authors, here in this paper research and for comparison purposes we will focus on three categories of these methods: standard methods [4], deoxyribonucleic acid (DNA) methods [5], and chaotic and hybrid methods. Standard methods such as data encryption standard (DES), advance encryption standard (AES) and blowfish (BF) provide a moderate speed; the fastest of them is BF method. Researchers [6] provided a BDNA method to enhance the speed of DNA based methods. Chaotic and hybrid method were introduced to enhance the security and speed of data cryptography, some of these methods increased the speed to 911 K bytes per second [7]-[16], and this was a good achievement provided by the chaotic based methods.

The existing methods of data cryptography share some feature, and many of these features can be considered as weak points, and the require enhancement, below these features will be listed, and the aims of the proposed method to enhance some of these features will be mentioned:

– Rounds

The existing methods require a lot of rounds in the encryption and decryption phases, these rounds start from 10 rounds for AES method and end with 16 rounds for BF [4]-[6]. Each round requires a secret key and all rounds must be executed. The proposed method will replace these rounds by layers, the number of layers will be variable and it must be selected by the user, they are independent and the output message of each layer can be taken as an encrypted-decrypted message.

– Speed

The existing method varied in speed, some of them provide a low speed (such as DES method), and other provide a good speed such as the chaotic method proposed in [5]. The proposed playing cards shuffling (PCS) method will increase the speed and it will provide a good speed up comparing with existing methods [17]-[26].

– Data blocking

The existing method support data dividing into block, the block size (BS) is small and fixed, the proposed PCS method will support data blocking using small a big blocks, the BS will be variable.

– Security level

The existing methods use a private key (PK) with length from 56 to 448 bits, some of these methods is not secure, others like AES and BF method provide a good level of security. The proposed PCS method will use a PK with a variable length; the length of the PK will depend on the number of selected layers.

– Simplicity and complicity

Each of the existing methods requires a complicated sequence of logical and arithmetic operations, this sequence must be executed in each round, the proposed PCS method will eliminate this sequence replacing it will simple blocks shuffling and shuffling back operations [27]-[36].

The aim of the paper is to produce an efficient and simplified method of data cryptography using playing cards shuffling operations, the method as it will be shown in the obtained results will speed up the process of cryptography comparing with existing standard and chaotic methods keeping the quality of the method acceptable and providing a high level of security by using a long PK. The proposed method will be implemented in a selected independent number of layers, each layer will totally encrypt-decrypt the message, increasing the number of layers will increase the security level of the PCS method. The method will be implemented in a variable number of layers. A layer is one function call of the encryption-decryption function. Each function will divide the input message into blocks; the block will be shuffled based on a generated indices key, formed by sorting a chaotic logistic key. The developed crypto system contains two parts: sender part, this part uses the encryption function to manipulate the source message and the PK to produce a cipher (encrypted message); receiver part, this part manipulates the cipher message and the PK to produce a decrypted message. The suggested method the suggested method will satisfy the following requirements of good crypto system:

– Security

Data hackers must be blocked by not being able to read the secret message or benefit from it in any way, this can be achieved by using a complicated private, this key must have a wide length, which will be able to produce a huge key space, that make the key strong enough to resist any hacking attack, the produced decrypted message must be sensitive to the selected values of the PK.

– Quality

The encrypted message must be completely destructive so that it cannot be used by any third party who is not authorized to view the message. The quality parameters values calculated between the source and the cipher messages must satisfy the quality requirements listed in Table 1. The decrypted message must be the same as the source message, the computed quality parameters values are to meet the quality requirements shown in Table 1.

Table 1. Quality parameters requirements

Quality parameter	Between source and decrypted message	Between source and encrypted message
Mean square error (MSE)	0	High
Peak signal to noise ratio (PSNR)	Infinite	Low

– Speed

The required times to implement each of the encryption and decryption algorithms must be minimized, thus the throughputs of message encryption and message decryption must be maximized.

– Simplicity

The number of used operations to execute each of the encryption and decryption algorithms must be reduced, the method must use a simple procedure to generate the required secret keys, the number of rounds must be reduced, and the complex sequence of logical and arithmetic operations used in the method must be reduced or eliminated.

2. THE PROPOSED PLAYING CARDS SHUFFLING METHOD

Standard base method require a few number of rounds, each round will require a complicated sequence of logical and arithmetic operations, making these methods sophisticated. The proposed method eliminates all these operations replacing them with a simple data values reordering, and employs one or more layers to encrypt-decrypt the secret message, each layer will be independent and the generated encrypted message in the layer may be considered as a final encrypted version. Figure 1 shows two layers of encryption, in each layer message encryption function (MEF) is called by using the parameters (message and layer PK which consist of one pair of chaotic logistic map (r and x) and the number of message blocks (NB).

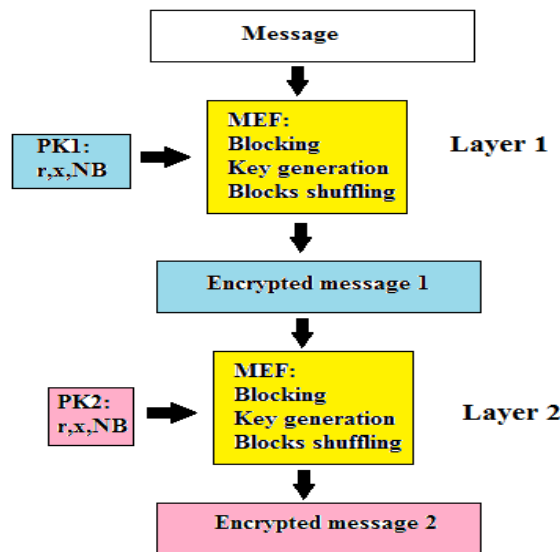


Figure 1. Two layers of encryption

This research applies 4 layers, where number of layers can be decreased or increased depending on the use wish. Increasing the number of layers will increase the security level. The PK will be complicated and the length of this key will depend on the selected number of layers, as example for 4 layers the length of the key will be calculated using (1), this key will provide a huge key space capable to resist any hacking attacks (see (2)).

$$PK \text{ length} = 4 \times 3 \times 64 = 768 \text{ bits} \quad (1)$$

$$Key \text{ space} = 2^{786} \\ 1.5525180923007089351489794884625 \times 10^{231} \text{ combinations} \quad (2)$$

The decryption function must use the same PK used in the encryption function, the produced decrypted message is very sensitive to the selected values of the PK, any minor changes in them in the decryption function will be considered as a hacking attempt by producing a damaged decrypted message.

The encryption function will perform two operations as shown below: indices key (IK) generation and message blocks shuffling. The IK generation task uses the parameters r , x , and NB to run a chaotic logistic map model to generate a chaotic key, then this key will be sorted to form the IK. The message blocks shuffling uses the NB value and the calculated BS to shuffle the message blocks based on the contents of IK. The encryption Algorithm 1 will use the following MEF written in MATLAB code: `function [EM] = Message_arrangement (m,NB,rl,x1);`

```

%Inputs:
%m:source message
%NB:number of blocks
%rl and x1:chaotic logistic parameters
%Output:
%ERM:Encrypted message
L=length(m);
BS=fix(L/NB);
for i=1:NB
    x1=x1*rl*(1-x1);    IK generation
    CK(i)=x1;
end
[qq IK]=sort(CK);
a1=m;
for i=1:NB
    c=IK(i);            Blocks shuffling
    a1((i-1)*BS+1:i*BS)=m((c-1)*BS+1:c*BS);
end
EM=a1;
end

```

Shuffling and shuffling back operations can be easily implemented using the IK contents, the blocks in the shuffling operation are taken depending on the contents of IK, while in the shuffling back operation the IK contents will be used as an index of blocks to be taken, the smallest index will be taken first, then the second smallest and so on, Figure 2 illustrates an example of how to execute these operations.

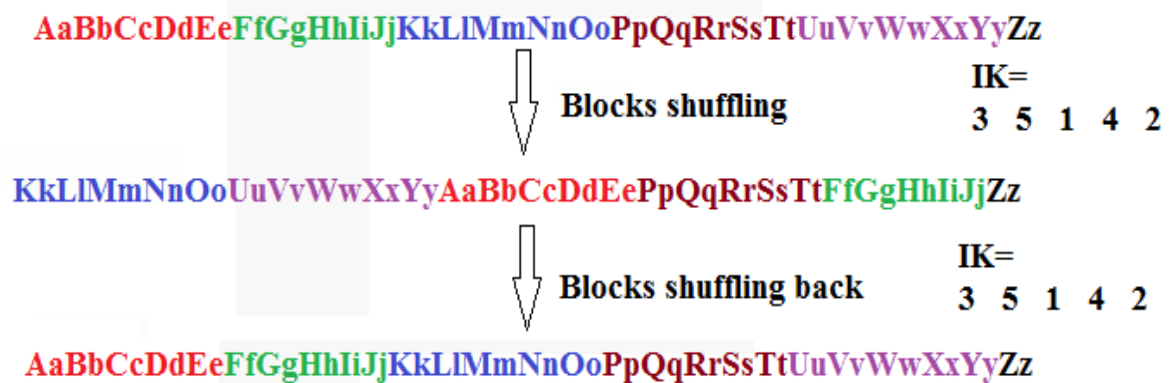


Figure 2. Shuffling and shuffling back operations implementation (example)

The decryption Algorithm 2 will be implemented in the same manner by replacing the shuffling operation with shuffling back operation as shown in the following MATLAB code:

```

function [DM] = Message_arrangement_R(m,NB,rl,x1);
Inputs:
%m: encrypted message
%NB:number of blocks
%rl and x1: Chaotic logistic parameters
%Output:
%DM:decrypted message
L=length(m);
BS=fix(L/NB);
for i=1:NB
    x1=x1*rl*(1-x1);    IK generation
    CK(i)=x1;
end
[qq IK]=sort(CK);
a1=m;
for i=1:NB
    c=IK(i);            Message shuffling back
    a1((i-1)*BS+1:c*BS)=m((i-1)*BS+1:i*BS);
end
DM=a1;
End

```

3. IMPLEMENTATION AND RESULTS DISCUSSION

The previous listed MATLAB codes of the proposed algorithm were implemented using a CPU with specifications depicted in Figure 3. The proposed PCS method was implemented using various messages, the obtained encrypted messages were always damaged, while the obtained decrypted messages were always identical to the source messages, Figures 4 and 5 show samples of the method implementation using 4 layers:

```

Processor:           Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz  2.50 GHz
Installed memory (RAM):  4.00 GB
System type:          64-bit Operating System
Pen and Touch:         No Pen or Touch Input is available for this Display
  
```

Figure 3. CPU specifications

```

m =
Protecting secret message using PCAP method

m1 =                               Layer1
ret mesing PCAProtectsage using secP method

m2 =                               Layer2
ret mesing Pe usinCAProtg secP methoectsagd

m3 =                               Layer3
CAProtsing P methog secPret mee usinectsagd

m4 =                               Layer4
ret mee usinectsng P metCAProtsihog secPagd
  
```

Figure 4. Sample outputs of the encryption phase

```

m4 =
ret mee usinectsng P metCAProtsihog secPagd
m5 =                               Layer1
CAProtsing P methog secPret mee usinectsagd
m6 =                               Layer2
ret mesing Pe usinCAProtg secP methoectsagd
m7 =                               Layer3
ret mesing PCAProtectsage using secP method
m8 =                               Layer4
Protecting secret message using PCAP method
  
```

Figure 5. Sample outputs of the decryption phase

The quality of the encrypted and decrypted messages was examined using the quality parameters MSE and PSNR, a selected messages were implemented and the MSE and PSNR values between each source message and the encrypted one were calculated, in Figure 6 shows PKs which used, the first one PK1 for short messages, while the second one PK2 for long messages, and Table 2 shows the obtained quality results:

PK1:

r=[3.6785 3.8993 3.5830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=6;NB2=10;NB3=12;NB4=5;NB5=15;

PK2:

r=[3.6785 3.8993 3.5830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=100;NB2=200;NB3=300;NB4=5;NB5=400;

Figure 6. PKs used

Table 2. Proposed PCS method quality results

Message length (byte)	Type	MSE	PSNR
100	Short	11661	17.1070
250	Short	10776	17.8962
500	Short	11071	17.6260
Message length (K bytes)			
5	Long	10802	17.9500
10	Long	11215	17.5750
15	Long	10786	17.9655
25	Long	10845	17.9105
50	Long	1.0884	17.8749
100	Long	10817	17.9368
Remarks		High	Low

The obtained low values of PSNR and high values of MSE prove that the proposed PCS method satisfied the quality requirements of good crypto system. The sensitivity of the proposed PCS method was tested on a message of length 5 K bytes and encrypted using different PKs shown in Figure 7. The quality parameters of the decrypted messages were calculated and Table 3 shows the obtained results:

PK1:

r=[3.6785 3.8993 3.5830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=100;NB2=200;NB3=300;NB4=5;NB5=400;

PK2:

r=[3.6785 3.8993 3.5830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=100;NB2=250;NB3=300;NB4=5;NB5=400;

PK3:

r=[3.7785 3.8993 3.6830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=100;NB2=200;NB3=300;NB4=5;NB5=400;

PK4:

r=[3.6785 3.8993 3.7830 3.6852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.7953 0.0081 0.1110 0.6184 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=100;NB2=200;NB3=300;NB4=5;NB5=400;

PK5:

r=[3.8785 3.8993 3.5830 3.9852 3.5568 3.6192 3.7208 3.8909 3.5911 3.7163];

x=[0.6953 0.0081 0.4110 0.6884 0.6190 0.9527 0.6552 0.7726 0.7732 0.4404];

NB1=130;NB2=200;NB3=300;NB4=5;NB5=400;

Figure 7. PKs used decryption process

Table 3. PCS method sensitivity results

Used PK in the decryption phase	MSE between the source and the decrypted message	PSNR between the source and the decrypted message
PK1	0	Infinite
PK2	2.1149	103.3350
PK3	2.1865	103.0024
PK4	2.0632	103.5828
PK5	2.0581	103.6075

As shown in Table 2 making changes in the PK will make the MSE non zero, and will make the PSNR value not infinite, and this prove the sensitivity of the proposed PCS method. The speed of the proposed PCS method was examined, a set of messages were selected and were implemented using the proposed PCS method, the encryption time was calculated and compared with other methods times, and Table 4 shows the obtained results.

Table 4. Speeds comparisons

Message length (K characters)	BDNA	BF	AES	DES	DNA	Proposed PCS method
5	0.048	0.054	0.053	0.152	0.200	0.0103
10	0.066	0.074	0.081	0.283	0.483	0.0110
15	0.090	0.097	0.106	0.405	0.625	0.0120
20	0.106	0.130	0.172	0.571	0.972	0.0140
25	0.123	0.133	0.198	0.785	1.250	0.0153
30	0.149	0.170	0.218	0.955	1.487	0.0159
Average						
17.5000	0.0970	0.1097	0.1380	0.5252	0.8362	0.0131
Average throughput (K bytes per second)	180.4124	159.5260	126.8116	33.3206	20.9280	1335.9
Speed up of the proposed PCS method	7.4047	8.3742	10.5345	40.0923	63.8331	1.0000
Speed up of PCS method equal throughput of PCS method divided by other method throughput (times)						

From Figure 8, it is shown that the smallest encryption time was provided by the proposed PCS method. PCS method maximized the throughput of message cryptography and provided a good speed up. The speed results of the proposed PCS method were compared with the speed results of other faster methods, and here the proposed method provided a good speed up as shown in Table 5.

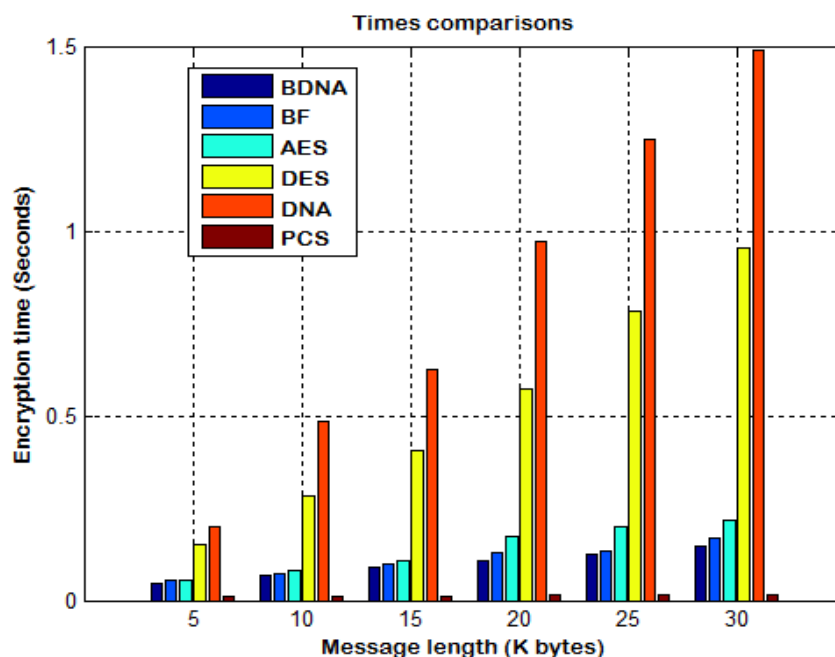


Figure 8. Methods encryption time comparisons

Table 5. Comparisons with other faster methods

Method	Throughput (K bytes per second)	Speed up of PCS method
Introduced in [6] hybrid	888.8867	1.5029
Introduced in [7] chaotic	638.4082	2.0925
Introduced in [8] chaotic	911.0352	1.4664
Introduced in [9] mixed DNA and chaotic	360.4102	3.7066
Introduced in [10] hybrid	384.9609	3.4702
Proposed PCS chaotic	1335.9	1.0000

4. CONCLUSION

A highly secure method of message cryptography PCS method was proposed, this level can be controlled by the selecting number of layers, increasing the number of layers increased the length of the PK, and thus increased the security level. PCS method provided a high speed of message cryptography, and it provided a good speed up comparing with standard methods, DNA based method and chaotic method. The proposed method enhanced the major features of the existing methods. The proposed PCS method used a variable message BS, replaced the rounds by layers, and each layer was an independent task, each layer can be used as a final layer. The proposed PCS simplified the processes of key generations by using a simple chaotic logistic map model to generate the required secret keys. The proposed method simplified the encryption and decryption processes by eliminating the complex of logical and arithmetic operation used in other methods by simple shuffling and shuffling back operations. The proposed method was tested and implemented using various messages, the obtained results proved the quality, sensitivity and efficiency of the proposed method. For future work the method could be used in banking systems and mobile applications.

ACKNOWLEDGEMENTS

The authors of this paper would like to acknowledge both Al-Balqa Applied University and Palestine Ahliya University for their kindness and assistance that made it easy to conduct this research.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rashad J. Rasras	✓	✓		✓	✓		✓	✓	✓	✓		✓		
Mutaz Rasmi Abu Sara		✓	✓			✓				✓	✓			
Ziad Alqadi	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓	

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**ding

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.




REFERENCES

- [1] Y. Manabe and H. Ono, "Card-Based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations," *New Generation Computing*, vol. 42, no. 3, pp. 305–329, Sep. 2024, doi: 10.1007/s00354-024-00257-2.
- [2] T. Mizuki and H. Shizuya, "A formalization of card-based cryptographic protocols via abstract machine," *International Journal of Information Security*, vol. 13, no. 1, pp. 15–23, Feb. 2014, doi: 10.1007/s10207-013-0219-4.
- [3] E. V. Haryanto, M. Zulfadly, Daifiria, M. B. Akbar, and I. Lazuly, "Implementation of Nihilist Cipher Algorithm in Securing Text Data with Md5 Verification," *Journal of Physics: Conference Series*, vol. 1361, no. 1, pp. 1–7, Nov. 2019, doi: 10.1088/1742-6596/1361/1/012020.
- [4] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in *Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005*, IEEE, 2005, pp. 84–89. doi: 10.1109/ICICT.2005.1598556.
- [5] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 1, pp. 1417–1425, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.024.
- [6] L. M. Heuchun Yepdia, A. Tiedeu, and G. Kom, "A Robust and Fast Image Encryption Scheme Based on a Mixing Technique," *Security and Communication Networks*, pp. 1–17, Feb. 2021, doi: 10.1155/2021/6615708.
- [7] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, Apr. 2019, doi: 10.1016/j.ins.2018.12.048.
- [8] M. Asgari-Chenaghlu, M. A. Balafar, and M. R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1–13, Apr. 2019, doi: 10.1016/j.sigpro.2018.11.010.
- [9] X. Zhang and X. Wang, "Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, Apr. 2019, doi: 10.1016/j.sigpro.2018.11.010.
- [10] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, May 2016, doi: 10.1016/j.optlaseng.2015.12.004.
- [11] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, Oct. 2016, doi: 10.1016/j.ijleo.2016.05.073.
- [12] D. S. A. Minaam, H. M. Abdual-Kader, and M. M. Hadhoud, "Evaluating the effects of symmetric cryptography algorithms on power consumption for different data types," *International Journal of Network Security*, vol. 11, no. 2, pp. 78–87, 2010.
- [13] S. Goldwasser and M. Bellare, "Lecture notes on cryptography," *Cryptography and Computer Security*, at MIT, no. July, pp. 1–289, 2008.
- [14] A. Kaushik, Satvika, M. Barnela, and A. Kumar, "Keyless User Defined Optimal Security Encryption," *International Journal of Computer and Electrical Engineering*, vol. 4, no. 2, pp. 99–103, 2012, doi: 10.7763/ijcee.2012.v4.458.
- [15] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: Des and AES," in *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science: Innovation for Humanity, SCEECS 2012*, IEEE, Mar. 2012, pp. 1–5. doi: 10.1109/SCEECS.2012.6184991.
- [16] M. Ebrahim, S. Khan, and U. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," *International Journal of Computer Applications*, vol. 16, no. 20, pp. 12–19, 2013, doi: 10.5120/10195-4887.
- [17] N. Kumar and P. Chaudhary, "Performance evaluation of encryption/decryption mechanisms to enhance data security," *Indian Journal of Science and Technology*, vol. 9, no. 20, pp. 1–10, May 2016, doi: 10.17485/ijst/2016/v9i20/70417.
- [18] A. H. Disina, Z. A. Pindar, and S. Jamel, "Enhanced Caesar Cipher to Exclude Repetition and Withstand Frequency Cryptanalysis," *Journal of Network and Information Security*, vol. 2, no. 1, pp. 112–117, 2015.
- [19] V. V. Palagushin, A. D. Khomonenko, and S. E. Adadurov, "Evaluation of cryptographic primitives security based on proximity to the Latin square," in *Conference of Open Innovation Association, FRUCT*, IEEE, Apr. 2016, pp. 266–271. doi: 10.1109/FRUCT-ISPIT.2016.7561537.
- [20] S. H. Jamel and M. M. Deris, "Diffusive primitives in the design of modern cryptographic algorithms," in *Proceedings of the International Conference on Computer and Communication Engineering 2008, ICCCE08: Global Links for Human Development*, IEEE, May 2008, pp. 707–710. doi: 10.1109/ICCCE.2008.4580696.
- [21] S. Manku and K. Vasanth, "Blowfish encryption algorithm for information security," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 10, pp. 4717–4719, 2015.
- [22] J. Daemen and V. Rijmen, "AES proposal: Rijndael," in *National Institute of Standards*, 1999, pp. 1–45.
- [23] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar, "An algebraic framework for Diffie-Hellman assumptions," *Journal of cryptology*, vol. 30, pp. 242–288, 2017, doi: 10.1007/978-3-642-40084-1_8.
- [24] N. D. Jorstad and J. Landgrave T. Smith, "Cryptographic algorithm metrics," in *20th National Information Systems Security*, 1997, pp. 1–38.
- [25] M. Faheem, U. Akram, I. Khan, S. Nageeb, A. Shahzad, and A. Ullah, "Cloud Computing Environment and Security Challenges: A Review," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, pp. 1–13, 2017, doi: 10.14569/ijacsa.2017.081025.
- [26] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms," *International Journal of Digital Technology & Economy*, vol. 1, no. 2, pp. 127–134, 2016, doi: 10.26472/ijces.v1i1.20.
- [27] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.
- [28] R. J. Rasras, Z. A. Alqadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology and Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, doi: 10.48084/etasr.2380.
- [29] R. J. Rasras, M. R. A. Sara, and Z. Alqadi, "Efficient Method to Message-Image Cryptography Using Reordered Image-Key," *Traitement du Signal*, vol. 40, no. 1, pp. 235–240, Feb. 2023, doi: 10.18280/ts.400122.
- [30] R. J. Rasras, Z. Alqadi, M. R. A. Sara, and B. Zahran, "Developing new multilevel security algorithm for data encryption-decryption (MLS_ED)," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 6, pp. 3228–3235, Dec. 2019, doi: 10.30534/ijatcse/2019/90862019.
- [31] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 442–448, 2017, doi: 10.14569/ijacsa.2017.080659.




- [32] A. M. Alshahrani and S. Walker, "Implement A Novel Symmetric Block Cipher Algorithm," *International Journal on Cryptography and Information Security*, vol. 4, no. 4, pp. 1–11, 2014, doi: 10.5121/ijcis.2014.4401.
- [33] M. E. Smid and D. K. Branstad, "The Data Encryption Standard: Past and Future," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550–559, May 1988, doi: 10.1109/5.4441.
- [34] Federal Information Processing Standards Publication, "Data encryption standard (DES)," *Federal Information Processing Standards Publication (FIPSPUB 46-3)*, vol. 25, no. 10, pp. 1–22, 1999, doi: 10.1007/springerreference_197.
- [35] R. J. Rasras, M. R. A. Sara, and Z. Alqadi, "Enhanced Efficiency and Security in LSB2 Steganography: Burst Embedding and Private Key Integration," *Traitement du Signal*, vol. 40, no. 5, pp. 1795–1805, Oct. 2023, doi: 10.18280/ts.400502.
- [36] M. M. Abu-Faraj and Z. A. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," *IJCSNS International Journal of Computer Science and Network Security*, vol. 21, no. 12, pp. 53–60, 2020.

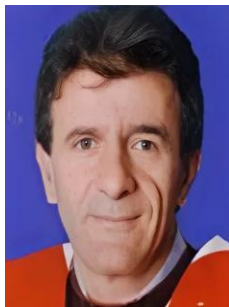
BIOGRAPHIES OF AUTHORS






Rashad J. Rasras    received the Ph.D. degree from National Technical University (Kharkov Polytechnic Institute) 2001, with research in automated intelligent control systems. Currently, He is an associate professor at Department of Electrical Engineering, Al-Balqa' Applied University. His research interests include image processing, machine learning, signal processing, and advanced computer architecture. He can be contacted at email: rashad.rasras@bau.edu.jo.



Mutaz Rasmi Abu Sara    received the Master's degree in computer science (database systems) in 2006 and Ph.D. from Saint Petersburg Electro technical University in 2010 with research and development of integrated database circuit components for CAD schematic, his research interest includes database systems, algorithms and machine learning. 2011-2020 he worked as assistant professor at Taibah University in K.S.A, currently he works as assistant professor at Palestine Ahliya University. He can be contacted at email: mutaz_abusara@yahoo.com.



Ziad Alqadi    received the Ph.D. degree from National Technical University (Kiev Polytechnic Institute) 1986 with research in parallel computer architecture. Currently, he is a professor at Department of Electrical Engineering, Al-Balqa' Applied University. His research interests include signal processing, parallel processing, and image processing. He can be contacted at email: natalia_maw@yahoo.com.